A New Algorithm for Computing Primitive Elements in *GF* (q^2)

I. S. Reed
University of Southern California

T. K. Truong and R. L. Miller
Tracking and Data Acquisition Engineering

A new method is developed to find primitive elements in the Galois field of q^2 elements $GF(q^2)$, where q is a Mersenne prime. Such primitive elements are needed to implement transforms over $GF(q^2)$.

I. Introduction

Several authors (Refs. 1 and 10) have proposed the use of the fast Fourier transform (FFT) over finite fields or rings. Such transforms can be used to compute circular convolutions of real sequences without round-off error. In Ref. 5, the authors extended the integer transforms of Rader by defining a complex number-theoretic transform over the Galois field $GF(q^2)$, where $q = 2^p - 1$ is a Mersenne prime for $p = 2, 3, 5, 7, 13, 17, 19, 31, 61, \cdots$. An algorithm was developed to compute elements of order 2^k for $1 \leqslant k \leqslant p + 1$. With this, an FFT algorithm of length 2^k was developed over $GF(q^2)$. Recently, the authors in Refs. 11 and 12 stated without proof the following result:

Let $GF(q^2)$ be a Galois field, where q is a Mersenne prime. If $d|(q^2 - 1)$, where $d = 2^k \cdot m$, m odd, $3 \leqslant k \leqslant p + 1$, and where $p|m$ for $p \leqslant m \leqslant 2^{p-1} - 1$, then there exists a generator α of the multiplicative subgroup G_d of order d, such that α satisfies

$$\alpha^{d/8p} \equiv (1 + \hat{i}) \bmod q$$

$$\alpha^{d/8} \equiv \text{one of forms } \pm 2^{(p-1)/2} (1 \pm \hat{i}) \bmod q$$

$$\alpha^{d/4} \equiv \hat{i} \text{ or } -\hat{i} \bmod q$$

and

$$\alpha^{d/2} \equiv -1 \bmod q \tag{1}$$

Using the above properties in $GF(q^2)$, a mixed high-radix transform of $2^k \cdot p$ points over $GF(q^2)$, where $3 \leqslant k \leqslant p+1$, can be developed. Such an algorithm for $GF(q^2)$ appears comparable in speed to that given by Winograd (Ref. 13).

In this article, a new method is presented for finding the primitive elements of $GF(q^2)$. Also a technique for finding an element of order d that satisfies Eq. (1) is given.

II. An Algorithm for Finding Primitive Elements in GF (q^2) where q is a Mersenne Prime

If q is a Mersenne prime, the order t of the multiplicative group with generator α of $GF(q^2)$ factors as follows:

$$t = (2^p - 1)^2 - 1 = 2^{p+1}(2^{p-1} - 1)$$

To find a primitive element of $GF(q^2)$, the following theorem is important.

Theorem 1: If q is a prime number, $t = q^n - 1$ and $t = p_1^{e_1} p_2^{e_2} \cdots p_k^{e_k}$, where the p_i are distinct primes, then γ is a primitive element of $GF(q^n)$, if and only if γ satisfies the congruences

$$\gamma^{t/p_1} \not\equiv 1 \bmod q \qquad (2)$$

$$\gamma^{t/p_2} \not\equiv 1 \bmod q$$

$$\vdots$$

$$\gamma^{t/p_k} \not\equiv 1 \bmod q$$

Proof: If γ is a primitive element of $GF(q^2)$, then $t = q^n - 1$ is the smallest positive number such that $\gamma^t \equiv 1 \bmod q$. Thus γ satisfies the congruences of Eq. (2).

Now assume γ satisfies congruences Eq. (2) and that $t = q^n - 1$ is not the smallest positive number for which this is true. Then there exists an integer ℓ for which $1 < \ell < t$ and $\ell \mid t$ such that $\gamma^\ell \equiv 1 \bmod q$. But when we have

$$\frac{t}{\ell} = p_i u$$

for some u and prime p_i in the factorization of t. Thus $t/p_i = \ell u$. Hence $\gamma^{t/p_i} \equiv 1 \bmod q$. This is contrary to assumption.

If q is a Mersenne prime, then $t = q^2 - 1 = 2^{p+1}(2^{p-1} - 1) = 2^{p+1} \cdot p_2^{e_2} \cdot p_3^{e_3} \cdots p_k^{e_k}$, where $p_i \neq p_j$ for $i \neq j$. Assume $\gamma = a + \hat{i}b$ is a primitive element of $GF(q^2)$. Then, by Theorem 1, γ satisfies

$$\gamma^{\frac{q^2-1}{p_1}} \equiv \gamma^{(2^{p+1}(2^{p-1}-1))/2} \equiv \gamma^{2^p(2^{p-1}-1)} \not\equiv 1 \bmod q$$

$$\gamma^{\frac{q^2-1}{p_2}} \equiv \gamma^{2^{p+1} \cdot p_2^{e_2-1} p_3^{e_3} \cdots p_k^{e_k}} \not\equiv 1 \bmod q$$

$$\vdots$$

$$\gamma^{\frac{q^2-1}{p_k}} \equiv \gamma^{2^{p+1} p_2^{e_2} \cdot p_3^{e_3} \cdots p_k^{e_k-1}} \not\equiv 1 \bmod q \qquad (3)$$

Since $q = 2^p - 1$, it is easily seen that

$$\gamma^{2^p} \equiv (a + \hat{i}b)^{2^p} \equiv (a + \hat{i}b)(a + \hat{i}b)^q$$

$$\equiv (a + \hat{i}b) \sum_{k=0}^{q} \binom{q}{k} a^{q-k} (\hat{i}b)^k \equiv (a + \hat{i}b)(a^q + (\hat{i}b)^q) \bmod q$$

By Fermat's theorem,

$$(a + \hat{i}b)(a^q + (\hat{i}b)^q) \equiv (a + ib)(a + \hat{i}^q b) \bmod q$$

But since $q \equiv 3 \bmod 4$,

$$\gamma^{2^p} \equiv (a + \hat{i}b)(a - \hat{i}b) \equiv a^2 + b^2 \bmod q$$

Thus Eq. (3) becomes

$$\gamma^{\frac{q^2-1}{p_1}} \equiv (a^2 + b^2)^{2^{p-1}-1} \equiv (a^2 + b^2)^{\frac{q-1}{2}} \not\equiv 1 \bmod q$$

$$\gamma^{\frac{q^2-1}{p_2}} \equiv (a^2 + b^2)^{2 \cdot p_2^{e_2-1} \cdot p_3^{e_3} \cdots p_k^{e_k}} \equiv (a^2 + b^2)^{\frac{q-1}{p_2}}$$

$$\not\equiv 1 \bmod q$$

.

.

.

$$\gamma^{\frac{q^2-1}{p_k}} \equiv (a^2 + b^2)^{2 \cdot p_2^{e_2} \cdot p_3^{e_3} \cdots p_k^{e_k-1}} \equiv (a^2 + b^2)^{\frac{q-1}{p_k}}$$

$$\not\equiv 1 \bmod q \tag{4}$$

By Theorem 1, the element $a^2 + b^2$ that satisfies Eq. (4) must be a primitive element of $GF(q)$. Thus if one can find a primitive element c in $GF(q)$ such that $c^{(q-1)/p_i} \equiv 1$ for $i = 1, 2, \cdots, k$, then the problem of finding a primitive element of $GF(q^2)$ is reduced to the problem of solving the congruence

$$a^2 + b^2 \equiv c \bmod q \tag{5}$$

for a and b.

To solve Eq. (5) let $X \equiv a^2 \bmod q$ and let $Y \equiv -b^2 \bmod q$. Then Eq. (5) becomes

$$X - c \equiv Y \bmod q \tag{6}$$

Proposition: Let $c \in GF(q)$, then there exist $a, b \in GF(q)$ such that $c = a^2 + b^2$.

Proof: If $q = 2^m$, then since $c^{2^m} = c$, it follows that $c = (c^{2^{m-1}})^2 + 0^2$. If q is odd, then

$$GF(q) = \{0, a_1, \cdots, a_{(q-1)/2}\}$$

$$\cup \{-a_1, -a_2, \cdots, -a_{(q-1)/2}\}$$

It is readily seen that there are exactly $(q + 1)/2$ elements of the form a^2 in $GF(q)$, and that there are $(q + 1)/2$ elements of the form $c - b^2$ for a fixed $c \in GF(q)$. Thus

$$\{a^2 \mid a \in GF(q)\} \cap \{c - b^2 \mid b \in GF(q)\} \neq \emptyset$$

Consequently we can express $c = a^2 + b^2$.

By the Proposition, one can choose the numbers X and Y from the set of integers $1, 2, \cdots, 2^p - 2$, such that X is a square and $Y = X - c$ is a nonsquare. Thus it is sufficient to let

$$a^2 \equiv X \bmod q$$

$$b^2 \equiv -X + c \equiv -Y \bmod q \tag{7}$$

By a procedure precisely similar to that used to find the solutions of congruence Eq. (14) in Ref. 5, the solutions of congruence (7) are given by

$$a \equiv \pm X^{2^{p-2}} \bmod 2^p - 1$$

$$b \equiv \pm(-Y)^{2^{p-2}} \bmod 2^p - 1 \tag{8}$$

The following theorem is often useful for finding solution of Eq. (5).

Theorem 2: If 3 is a primitive element of $GF(q)$, then the solution of the congruence

$$a^2 + b^2 \equiv 3 \bmod q$$

for a and b are given by

$$a = (2^{\frac{p-1}{2}} + 1)$$

and

$$b = (2^{\frac{p-1}{2}} - 1)$$

Proof: Note that $3 \equiv 2^p - 1 + 3 \bmod q$. Thus

$$3 \equiv 2^p + 2 \equiv (2^{\frac{p-1}{2}} + 1)^2 + (2^{\frac{p-1}{2}} - 1)^2$$

$$\equiv a^2 + b^2 \bmod q$$

and

$$a = 2^{\frac{p-1}{2}} + 1$$

$$b = 2^{\frac{p-1}{2}} - 1$$

are identically the solutions of the congruence.

To find a solution of $x^c \equiv 1 + \hat{i} \bmod q$ where $c = 2^k \cdot m/8p$, assume $\gamma = a + \hat{i}b$ is a primitive element of $GF(q^2)$. Then, using a computer program, one can find an integer j such that $\gamma^j \equiv 1 + \hat{i} \bmod q$. Hence

$$(\gamma^j)^{(q^2-1)/c} \equiv (1 + \hat{i})^{(q^2-1)/c}$$

$$\equiv ((1 + \hat{i})^{8p})^{(q^2-1)/2^k \cdot m} \bmod q \qquad (9)$$

where $2^k \cdot m \mid q^2 - 1$.

It was shown in Ref. 12 that the element $(1 + \hat{i})$ is an element of order $8p$ in $GF(q^2)$. Thus Eq. (9) becomes

$$(\gamma^j)^{(q^2-1)/c} \equiv 1 \bmod q$$

Since γ is primitive, this implies $c \mid j$. Thus

$$(\gamma^{j/c})^c \equiv (1 + \hat{i}) \bmod q$$

where $c = 2^k \cdot m/8p$ for $3 \leqslant k \leqslant p - 1$, where $p \mid m$ for $p \leqslant m \leqslant 2^{p-1} - 1$. Hence, $\alpha = \gamma^{j/c}$ is an element of order $d = 2^k \cdot m$ in $GF(q^2)$ such that α satisfies (1).

Consider a simple example:

Example 1: Let $q = 2^p - 1 = 2^3 - 1$. Then $q^2 - 1 = 2^{p+1}(2^{p-1} - 1) = 2^4 \cdot 3$. Find an element $\alpha = a + \hat{i}b$ of $GF(7^2)$ such that satisfies

$$\alpha^{(q^2-1)/8p} \equiv \alpha^{48/24} \equiv \alpha^2 \equiv (1 + \hat{i}) \bmod q$$

$$\alpha^{48/8} \equiv \alpha^6 \equiv 2(-1 + \hat{i}) \bmod q$$

$$\alpha^{48/4} \equiv \alpha^{12} \equiv -\hat{i} \bmod q$$

$$\alpha^{48/2} \equiv \alpha^{24} \equiv -1 \bmod q$$

First we note that 3 satisfies the congruences:

$$3^{\frac{7-1}{2}} \equiv -1 \not\equiv \bmod 7 \qquad (10)$$

and

$$3^{\frac{7-1}{3}} \equiv 3^2 \equiv 2 \not\equiv 1 \bmod 7$$

Thus by Theorem 1, 3 is a primitive element of $GF(7)$. Using Eq. (10) in Eq. (4) and Eq. (5) the problem of finding a primitive element in $GF(q^2)$ is reduced to the solution of the congruence,

$$a^2 + b^2 \equiv 3 \bmod 7 \qquad (11)$$

By Eq. (6) the solution of Eq. (11) is equivalent to the solution of

$$X - 3 \equiv Y \bmod 7$$

where $X \equiv a^2 \bmod 7$ and $Y \equiv -b^2 \bmod 7$. It can be shown that $Y = 6$ is nonsquare and $X = Y + 3 = 9$ is a square. Thus, by Eq. (7),

$$a^2 \equiv 9 \equiv 2 \bmod 7$$

$$b^2 \equiv -6 \equiv 1 \bmod 7 \qquad (12)$$

Hence by Eq. (8), the solution of congruence (12) are given by

$$a \equiv -2^{2^{p-2}} \equiv -2^2 \equiv 3 \bmod 7$$

$$b \equiv (1)^{2^{p-2}} \equiv (1)^3 \equiv 1 \bmod 7$$

Note that since $c = 3$ in Eq. (11), the solution of the congruence Eq. (11) can be also obtained by using Theorem 2. It is evident that Theorem 2 yields the same solution, as follows:

$$a \equiv (2^{\frac{p-1}{2}} + 1) = 2^{\frac{3-1}{2}} + 1 = 3$$

$$b \equiv 2^{\frac{p-1}{2}} - 1 = 2^{\frac{3-1}{2}} - 1 = 1$$

Hence $\gamma = -4 + \hat{i}$ is a primitive element of $GF(7^2)$. Since $(1 + \hat{i})^{48/2} \equiv (1 + \hat{i})^{24} \equiv 1 \bmod q$, then $x^2 \equiv 1 + \hat{i}$ has a solution. To find such a solution it is necessary to find an integer j such that $\gamma^j \equiv 1 + \hat{i} \bmod q$. In this case, $j = 14$, i.e., $\gamma^{14} \equiv 1 + \hat{i} \bmod q$. Thus

$$(\gamma^{14/2})^2 \equiv 1 + \hat{i} \bmod q$$

Hence $\gamma^{14} \equiv 1 + \hat{i} \bmod q$ and the desired element is $\alpha = \gamma^7$ of order 48 in $GF(7^2)$. Evidently $\alpha = \gamma^7$ satisfies also

$$\alpha^6 \equiv (1 + \hat{i})^3 \equiv 2(-1 + \hat{i}) \bmod q$$

$$\alpha^{12} \equiv -\hat{i} \bmod q$$

and

$$\alpha^{24} \equiv -1 \bmod q$$

With the same procedure used in Example 1 and then using a computer program, the primitive elements for a number of different Mersenne primes were found. These are shown in Table 1.

Acknowledgment

The authors wish to thank Dr. N. A. Renzetti, Manager of Tracking and Data Acquisition Engineering, and the members of the Advanced Engineering Group in that organization at the Jet Propulsion Laboratory for their early support, suggestions and encouragement of the research which led to this paper. We also thank Dr. C. A. Greenhall for his computer programming assistance.

References

1. Pollard, J. M., "The Fast Fourier Transform in a Finite Field," *Math. Comput.*, 1971, 25, pp. 365–374.
2. Schonhage, A., and Strassen, V., "Schnelle Multiplikation Grosser Zahlen," *Computing*, 1971, 7, pp. 281–292.
3. Rader, C. M., "Discrete Convolution via Mersenne Transforms," *IEEE Trans.*, 1972, C-21, pp. 1269–1273.
4. Agarwal, R. C., and Burrus, C. S., "Number Theoretic Transforms to Implement Fast Digital Convolution," *Proc. IEEE*, 1975, 63, pp. 550–560.
5. Reed, I. S., and Truong, T. K., "The Use of Finite Fields to Compute Convolutions," *IEEE Trans.*, 1975, IT-21, pp. 208–213.
6. Reed, I. S., and Truong, T. K., "Complex Integer Convolution Over a Direct Sum of Galois Fields," *ibid*, 1975, IT-21, pp. 657–661.
7. Vegh, E., and Leibowitz, L. M., "Fast Complex Convolution in Finite Rings," *ibid*, 1976, ASSP-24, pp. 343–344.
8. Golomb, S. W., Reed, I. S., and Truong, T. K., 'Integer Convolutions Over the Finite Field GF($3 \cdot 2^n + 1$)," *SIAM J. Appl. Math.*, Vol. 32, No. 2, March 1977.
9. Pollard, J. M., "Implementation of Number-Theoretic Transforms," *Electron. Lett.*, 1976, 12, pp. 378–379.
10. Liu, K. Y., Reed, I. S., and Truong, T. K., "Fast Number-Theoretic Transforms for Digital Filtering," *ibid*, 1976, 12, pp. 644–646.
11. Reed, I. S., Truong, T. K., and Liu, K. Y., "Fast Algorithm for Computing Complex Number-Theoretic Transforms," *Electronics Letters*, 12th May 1977, 13, No. 10, pp. 278-280.
12. Reed, I. S., and Truong, T. K., "Addendum to Fast Algorithm for Computing Complex Number-Theoretic Transforms," to be published in *Electronics Letters*.
13. Winograd, S., "On Computing the Discrete Fourier Transform," *Proc. Nat. Acad. Sci. USA*, 1976, 73, pp. 1005–1006.
14. Vinogrador, I. M., *Elements of Number Theory*, Dover Publications, New York, 1954.

Table 1. Primitive elements of $GF(q^2)$ for different q

	$q = 2^p - 1$	Primitive element of $GF(q)$	$a^2 + b^2 \bmod q$	Primitive element of $GF(q^2)$
3	7	3	$3^2 + 1^2$	$3 + \hat{i}$
5	31	3	$5^2 + 3^2$	$5 + \hat{i}\,3$
7	127	3	$9^2 + 7^2$	$9 + i\,7$
13	32767	17	$4^2 + 1^2$	$4 + \hat{i}$
17	131071	3	$257^2 + 255^2$	$257 + \hat{i}\,255$
19	524287	3	$513^2 + 511^2$	$513 + \hat{i}\,511$
31	2147483647	53	$7^2 + 2^2$	$7 + \hat{i}\,2$